Lecture 10-14: Tensor products II

October 14, 2024

Perhaps not surprisingly, the tensor product of two modules with a product structure also has a product structure. I will exploit this to study certain rings that are also vector spaces over fields F, defining a product on certain equivalence classes of such rings that yields information about F.

Given a commutative ring R, an R-algebra is a ring A that is also an R-module such that $(ra)b = a(rb) = r(ab)$ for $r \in R, a, b, \in A$ (Definition, p. 342). Then we have

Proposition 21, p. 374

The tensor product $A \otimes_R B$ of two R-algebras A, B is again an R-algebra, satisfying $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$ for $a_i \in A, b_i \in B$.

The proof is a very simple calculation.

Today I want to concentrate on the special case where $R = F$ is a field and A and B are (finite-dimensional) central simple over F, so that the centers of A and B both coincide with the images of F inside them, A and B are finite-dimensional over F, and neither A nor B has a nonzero proper two-sided ideal. Then one has

Theorem

The tensor product $C = A \otimes_F B$ is central simple over F whenever A and B are.

Proof.

Any element of C can be written as $\sum_{i=1}^{m} a_i \otimes b_i$, with $a_i \in A, b_i \in B$, and the b_i linearly independent over F. If I is a nonzero proper ideal of C, choose a nonzero $x \in I$ of this form with m as small as possible. The ideal of A generated by a_1 must be all of A, so there are $d_1, \ldots, d_r, e_1 \ldots, e_r \in A$ with $\sum_i d_i a_1 e_i = 1$. Then $x' = \sum_i (d_i \otimes 1) x (e_i \otimes 1) = \sum_i a_i' \otimes b_i$ lies in I, has the same value of m as x, and has $a_1' = 1$. If $a_i' \notin F$ for any $i \neq 1$, then we can take the commutator $(a \otimes 1)x' - x'(a \otimes 1)$ for suitable $a \in A$ to produce an element of I with a smaller value of m, a contradiction, unless $m = 1$. But then we have $1 \otimes b \in I$ for some nonzero $b \in B$; choosing $d_1' \ldots, d_s', e_1', \ldots, e_s' \in B$ with $\sum d_i' b e_i' = 1$ and forming the corresponding sum with b replaced by $1 \otimes b$, we get $1 \otimes 1 \in I$, a contradiction. □

Proof.

Thus C is simple. If $x = \sum a_i \otimes b_i$ has linearly independent b_i, lies in the center of C, and has $a_i \notin F$ for some i, then the commutator of x and $a \otimes 1$ for suitable $a \in A$ is not 0, since a sum $\sum a_i' \otimes b_i$ for $a_i' \in A$ can be 0 only if all a_i' are 0. So all a_i lie in F and one can replace x by $1 \otimes b$ for some $b \in B$. Taking the commutator with a suitable $1 \otimes b'$, one sees that b must lie in F, so that the center of C is F, as claimed. □

Thus the tensor product over F defines a product structure on the set of (isomorphism classes of) central simple algebras over F. By results proved last time, this product is commutative and associative. It has the algebra F as an identity element, since $F \otimes_F A \cong A$ for any F-algebra A. But inverses are lacking, since the dimension over F of any tensor product $A \otimes_F B$ is the product of the dimensions of A and B over F, so cannot be one unless A and B are both isomorphic to F.

To remedy this defect I will quote a basic result that any finite-dimensional central simple algebra A over a field F is isomorphic to the ring $M_r(D)$ of all $r \times r$ matrices over a central simple division algebra D over F; moreover, both D and r are uniquely determined by A (see the Example, p. 834, property III). Writing $A \sim B$ if the algebras A, B are matrix rings over the same division algebra D, one easily sees that $\sim$ is an equivalence relation. The above product is then well defined on $\sim$-equivalence classes.

Thus the central simple F-algebra A will have an inverse under the above product if there is an algebra B such that $A \otimes_F B \cong M_r(F)$ for some r. It turns out that there is a simple uniform recipe for such an algebra: setting $B = A$ as an F-vector space but with multiplication defined by the rule that the product of $a_1, a_2 \in B$ is the reverse product $a_2 a_1$ in A, then one easily checks that B is central simple. This B is denoted A^o and called the opposite algebra of A.

Theorem

With notation as above, one has $A \otimes_F A^o \cong M_r(F)$, where $r = \dim_F A$.

Proof.

Define a map from $C = A \otimes_F A^o$ to $M_r(F)$ by sending $\sum_i a_i \otimes a_i'$ to $\sum \lambda_{a_i} \rho_{a_i'}$, regarded as an F-linear transformation from A to itself, where λ_a, ρ_a respectively denote the ltransformations corresponding to left and right multiplication by a. This map is well defined on the tensor product and a homomorphism, thanks to the definitions of multiplication in C and the opposite algebra A_o. Since it is clearly not the 0 map and C is simple, it must have trivial kernel; since both C and $M_r(F)$ have dimension r^2 over F, it must be an isomorphism, as desired. □

The upshot of this discussion is to any field F we can attach a group, called its Brauer group and denoted $\mathrm{Br}(F)$, consisting of all equivalence classes of finite-dimensional central simple algebras over F, with multiplication given by tensoring over F (see the Definition on p. 836).

Example

If F is the field $\mathbb{C}$ of complex numbers, then the only central simple division algebra over F is F itself. This fact turns out to be a simple consequence of the Fundamental Theorem of Algebra that every polynomial in one variable over $\mathbb{C}$ is the product of linear factors. Consequently $\mathrm{Br}(\mathbb{C})$ is the trivial group. If F is a finite field, then $\mathrm{Br}(F)$ is also trivial; this is because a famous theorem of Wedderburn (which you will prove later) asserts that the only finite division rings are fields, so that again the only central simple division algebra over F is F itself.

Example

For the field $F = \mathbb{R}$ of real numbers matters are more interesting. There is a famous division algebra over F different from F, called the quaternions (or the Hamilton quaternions in the text on p. 224) and denoted $\mathbb{H}$. It is four-dimensional over F, having a basis denoted $1, i, j, k$; here you should think of i, j, k as the coordinate axes in $\mathbb{R}^3$, as in physics. Of course 1 is the multiplicative identity; the other basis elements multiply according to the rules $i^2 = j^2 = k^2 = -1, ij = -ji = k, ki = -ik = j, jk = -kj = i$. Bearing in mind the usual formula for dot and cross products in $\mathbb{R}^3$, one can check that any two real combinations v, w of i, j, k have the product $-(v \cdot w) + (v \times w)$ in $\mathbb{H}$, where of course $v \cdot w \in \mathbb{R}$ and $v \times w \in \mathbb{R}^3$ is the cross product of v and w, regarded as a linear combination of i, j, k.

Example

Defining the conjugate $\bar{z} = \overline{a + bi + cj + dk}$ of $z = a + bi + cj + dk$ as $a - bi - cj - dk$ (analogous to the complex conjugate), one finds that $\overline{zw} = \overline{w}\,\overline{z}$ (it is enough to check this for $v, w \in \{1, i, j, k\}$) and $N(z) = z\bar{z} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}$, with $N(z) = 0$ if and only if $z = 0$. Hence the multiplicative inverse z^{-1} exists in $\mathcal{H}$ if $z \neq 0$ and is given by $\frac{\bar{z}}{N(z)}$. The map sending $z \in \mathbb{H}$ to $\bar{z}$ defines an isomorphism between $\mathbb{H}$ and its opposite $\mathcal{H}^o$, so that the class of $\mathbb{H}$ is its own inverse in $\mathrm{Br}(\mathbb{R})$. In fact the classes of $\mathbb{R}$ and $\mathbb{H}$ are the only ones in $\mathrm{Br}(\mathbb{R})$, so that this group is cyclic of order two.

Example

Of course there is no need to insist on real coefficients of $1, i, j, k$ here. One could equally well consider all combinations $a + bi + cj + dk$ with $a, b, c, d \in \mathbb{Q}$, or even $a, b, c, d \in \mathbb{Z}$. The former choice leads to a central simple division algebra over $\mathbb{Q}$, but this time it turns out that there are many other such examples: $\mathrm{Br}(\mathbb{Q})$ is an infinite group (but still countable). What if one took the coefficients to lie in the finite field $\mathbb{Z}_p$ with p prime? At first it seems that one would get another division ring, but this cannot be the case, since I have already mentioned that all finite division rings are fields. Instead it turns out that the equation $a^2 + b^2 + c^2 + d^2 = 0$ always has a nontrivial solution in $\mathbb{Z}_p$, so the analogue of $\mathbb{H}$ over $\mathbb{Z}_p$ has zero divisors.